Comment l'état traite-t-il nos données ?

Jacques, Florian

Published in:
Espace de libertés

Publication date:
2022

Document Version
le PDF de l'éditeur

Florian Jacques
Assistant à la Faculté de droit de l'UNamur
et chercheur au NaDI/Crids

COMMENT L'ÉTAT TRAITE-T-IL NOS DONNÉES ?

Le numérique prend de plus en plus d'importance dans les relations entre État et citoyens. L'épidémie de Covid-19 a aussi mis en lumière le développement croissant d'outils tels que le *Covid Safe Ticket* (CST) et les applications de tracing qui reposent sur l'utilisation de données. Dans ce contexte, le citoyen peut se sentir démuni et avoir la sensation de perdre la maîtrise de ses données.

Dans bien des cas, il est peu aisé pour le citoyen de savoir quelles informations le concernant sont détenues par différentes autorités publiques, dans quels buts elles sont utilisées et où elles sont physiquement stockées. Face à ce constat, il est utile de rappeler que le droit contient déjà des possibilités permettant au citoyen de reprendre la main sur ses données à caractère personnel et d'identifier quelles autorités publiques les traitent. À ce titre, le règlement général sur la protection des données (ou RGPD) dote notamment les personnes concernées d'un droit d'accès pouvant être exercé vis-à-vis des autorités publiques. De même, une série d'outils et d'initiatives permettent déjà, dans une certaine mesure, une plus grande transparence. On mentionnera, à titre exemplatif, la plateforme Mon dossier du Registre national ainsi que les portails My Minfin et My Data Belgium.

Néanmoins, le risque de perte de maîtrise subsiste, en particulier quand des données ne sont pas traitées dans le strict respect des balises juridiques qui entourent les traitements de données par l'État. Il s'agit avant tout du principe constitutionnel de légalité en vertu duquel l'adoption d'une législation est requise pour instaurer un traitement de données. La loi doit en outre être suffisamment claire et contenir les principaux éléments du traitement tels que les données traitées, la finalité (c'est-à-dire le but poursuivi) ou les destinataires. À ces exigences s'ajoutent les principes de transparence et d'objectif inscrits dans le RGPD. L'importance de ces balises est illustrée ci-après au moyen d'exemples concrets

qui devraient, à l'avenir, susciter la vigilance de la société.

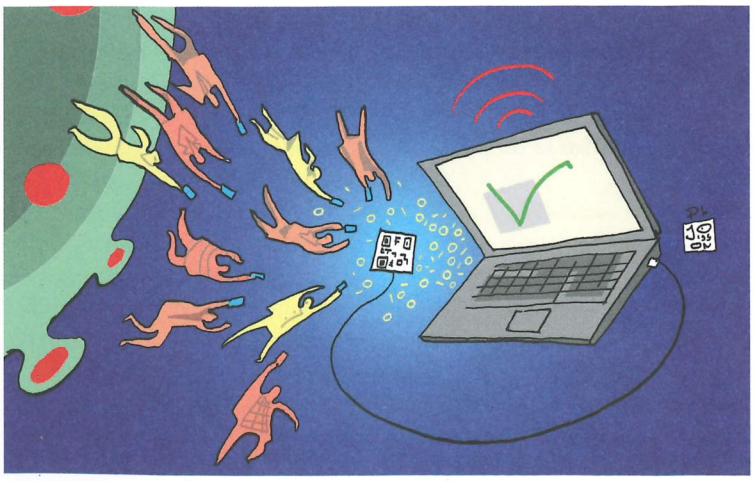
L'importance de l'intervention du législateur

Dans le chef du citoyen, la première source de perte de maîtrise de ses données résulte du non-respect du principe de légalité formelle. Dans ce cas, ses données sont traitées sans que les éléments essentiels du traitement aient été préalablement débattus par une assemblée parlementaire. La crise liée à la pandémie de Covid-19 a démontré une tendance à la multiplication des entorses à ce principe. Outre la collecte de données de contact dans l'Horeca organisée par un arrêté ministériel et une base de données relative à la vaccination initialement encadrée par un arrêté royal, il faut relever que la suspension temporaire d'un CST était prévue dans une norme de valeur réglementaire (à savoir un accord de coopération d'exécution). Bien que la volonté d'empêcher des personnes vaccinées mais contaminantes de pouvoir utiliser un CST soit légitime, il n'en reste pas moins que la création d'une liste identifiant les certificats vaccinaux de ces personnes est une finalité de traitement. Aussi, en tant qu'élément essentiel du traitement, celui-ci devait figurer dans une norme législative.

La nécessaire application rigoureuse du « principe de finalité »

Comme mentionné, la Constitution réserve à la loi le soin de définir les finalités d'un traitement. Au sens du RGPD, ces finalités doivent, de plus, être « déterminées, explicites et légitimes ». Derrière cette formulation se cache l'exigence d'identifier des objectifs de traitement clairs qui ne sont ni ambigus ni trop larges. Il s'agit là d'une étape cruciale dès lors qu'elle permet aussi de discerner qui est autorisé à accéder aux données. En effet, une fois l'objectif nettement défini il devient possible de savoir « qui » doit avoir accès aux données pour atteindre cet objectif.

Le récent décret wallon modifiant le Code wallon de l'action sociale et de la santé illustre cette problématique. Ce décret doit être pointé du doigt dans la mesure où il contient un mécanisme dont la prévisibilité doit être remise en question. En application de ce texte, à l'annonce d'une situation d'urgence épidémique fédérale, le gouvernement wallon est autorisé à déclarer l'urgence sanitaire. Dans cette hypothèse, il peut alors adopter toutes mesures pour « gérer, monitorer et maîtriser » une épidémie, en ce compris traiter des données, dans le but de mettre en place des mesures sanitaires adéquates. Force est de constater que cet objectif largement défini ne répond pas au standard de « finalité déterminée » du RGPD. En outre, il s'agit là d'une habilitation à imposer des traitements de données, potentiellement réalisés par des tiers, par voie réglementaire.



Des croisements de données trop peu encadrés

La troisième source de risque que nous identifions résulte des croisements de données. À ce sujet, le droit belge autorise tant les institutions de la Sécurité sociale que le SPF Finances à employer des outils numériques de détection de fraude. En pratique, la loi leur permet de collecter des données, de les injecter dans de grandes bases de données (ou *data warehouse*), de les croiser pour en extraire de nouvelles informations et de recourir à des techniques de profilage du citoyen.

Ici encore, la prévisibilité de la mise en œuvre de ces normes doit être remise en question pour plusieurs raisons. Tout d'abord, l'objectif poursuivi par le traitement de données est particulièrement large. Ensuite, il n'est pas précisé quelles sont les données traitées. Il en découle un risque évident de réutilisation de celles-ci hors du contexte dans lequel elles ont été collectées. Enfin, l'intervention du Comité de sécurité de l'information (CSI) est nécessaire.

Une délibération de cet organe, créé en 2018, est en effet requise pour autoriser d'une part les transferts de données entre institutions de la Sécurité sociale, et d'autre part, l'injection de données issues de tiers dans le *data warehouse* du SPF Finances[1]. Ce mécanisme n'est toutefois pas exempt de critiques puisque le Conseil d'État a épinglé le fait que l'adoption de délibérations – auxquelles les citoyens pour les citoyens dont les données sont traitées se trouvent liés – revenait à doter le CSI d'un pouvoir réglementaire. Pour autant, ces délibérations ne font l'objet d'aucun contrôle *a priori* par l'APD ou le Conseil d'État. De même, *a posteriori*, l'APD peut uniquement solliciter la modification des délibérations. Le recours en annulation par le Conseil d'État n'est pas non plus expressément consacré dans la loi relative au CSI.

Accroître la transparence des outils numériques

Enfin, un manque de transparence certain existe lors de la mise en œuvre concrète d'outils numériques dont l'utilisation est rendue obligatoire par l'État. Est ici particulièrement visée la question de savoir quelles entités, publiques ou privées, sont techniquement impliquées dans le traitement des données du citoyen. Bien évidemment, le droit n'interdit aucunement aux pouvoirs publics de faire appel aux services de sous-traitants informatiques spécialisés. Cela étant, l'identité de ces acteurs est souvent méconnue du citoyen. On relèvera par exemple que, pour le fonctionnement du CST, la liste des certificats de vaccination temporairement suspendus a été hébergée dans un *cloud* d'Amazon. Alors que le RGPD impose d'informer la personne concernée de l'identité des destinataires de données, le citoyen belge ne peut prendre connaissance de cette information qu'en consultant des documents techniques[2]. Il est pourtant raisonnable de supposer qu'il possède un intérêt légitime à disposer de ce renseignement, *a fortiori* lorsque les données traitées sont sensibles, que les GAFAM sont impliqués et qu'il ne peut choisir de se soumettre à ce traitement de données.

1 Voir à ce propos l'article 15, §1er de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la Sécurité sociale et l'article 5 de la loi du 3 août 2012 relative aux traitements de données à caractère personnel réalisés par le Service public fédéral Finances.

2 Il s'agit de l'AIPD relative aux applications COVIDsafe et COVIDscan. Voir « CovidScan applicatie België. Gegevensbeschermingseffectbeoordeling », v.02.02, p. 14, mis en ligne sur www.covidscan.be.